CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

OSINT

Open Source Intelligence (OSINT) znamená zber, analýzu a využívanie informácií z verejne dostupných zdrojov. Tento proces nachádza uplatnenie v rôznych oblastiach vrátane kybernetickej bezpečnosti, presadzovania práva, národnej bezpečnosti, podnikovej bezpečnosti, žurnalistiky a konkurenčného spravodajstva. OSINT môže zahŕňať informácie z internetu, sociálnych médií, diskusných fór, verejných záznamov a ďalších voľne prístupných zdrojov.

OSINT ZHROMAŽĎUJE ÚDAJE ZO ŠIROKEJ ŠKÁLY ZDROJOV VRÁTANE:

Uplatnenie v kybernetickej bezpečnosti je rozsiahle. Využíva sa na identifikáciu hrozieb, analýzu potenciálnych rizík a monitorovanie aktivít, ktoré môžu ohroziť bezpečnosť organizácie. OSINT pomáha odborníkom kybernetickej bezpečnosti získať prehľad o zraniteľnostiach systémov, sledovať aktivity útočníkov a dokonca predchádzať kybernetickým útokom tým, že identifikuje indikátory kompromitácie už v počiatočnom štádiu. Vo väčšine prípadov je vyžadované, aby analytik identifikoval a koreloval viacero údajových bodov na overenie hrozby pred prijatím opatrení. Efektívne využívanie OSINT môže byť rozhodujúcim faktorom pri ochrane aktív.

VÝHODY A NEVÝHODY OSINT

- **Zákonnosť:** OSINT zahŕňa používanie verejne dostupných zdrojov, vďaka čomu je legálne zhromažďovať informácie, v porovnaní s inými metódami, ktoré môžu zahŕňať zásah do súkromia alebo vyžadujú špeciálne povolenia.
- **Príliš mnoho informácií:** Obrovské množstvo dostupných údajov môže byť ohromujúce, čo sťažuje filtrovanie a zameranie sa na relevantné informácie bez pokročilých nástrojov a metodík.
- **Náklady:** Keďže používa otvorené zdroje, OSINT má vo všeobecnosti nižšie náklady ako skryté spravodajské metódy, ktoré si môžu vyžadovať špecializované vybavenie alebo personál.
- **Kvalita a spoľahlivosť:** Verejne dostupné informácie sa môžu značne líšiť v kvalite a spoľahlivosti s potenciálom dezinformácií, zaujatosti a nepresností.
- **Široká škála zdrojov:** OSINT môže čerpať z rôznych zdrojov vrátane spravodajských médií, sociálnych médií, akademických publikácií a vládnych správ, čím poskytuje široký pohľad na danú tému.
- **Nedostatok hĺbky:** OSINT môže prehliadať informácie, ktoré možno získať prostredníctvom tajných alebo súkromných zdrojov, čím môže prísť o kritické poznatky, ktoré nie sú verejné.
- **Dostupnosť:** Informácie sú ľahko dostupné komukoľvek s prístupom na internet, čo z nich robí flexibilný a prispôsobiteľný nástroj pre rôznych používateľov vrátane vládnych organizácií, firiem a jednotlivcov.
- **Fragmentácia:** Informácie môžu byť rozptýlené na rôznych platformách, čo si vyžaduje značné úsilie na zhromažďovanie a spracovanie do zrozumiteľných informácií.
- **Aktuálnosť:** Údaje v reálnom čase zo zdrojov, ako sú sociálne médiá, môžu poskytnúť informácie o aktuálnych udalostiach, trendoch a nových hrozbách.
- **Kompetencie a zručnosti:** Efektívny OSINT vyžaduje určitú úroveň odbornosti v oblasti analýzy údajov, kritického myslenia a znalosti rôznych nástrojov a technológií, ktoré nemusia byť ľahko dostupné pre všetkých používateľov.

VEDELI STE, ŽE ... ?

Moderný OSINT sa vo veľkej miere spolieha na platformy **sociálnych médií**. Analytici môžu sledovať udalosti v reálnom čase, nálady verejnosti a dokonca predpovedať budúce trendy monitorovaním platforiem ako Twitter, Facebook a Instagram.

OSINT zahŕňa aj **geopriestorovú inteligenciu** (GEOINT), kde analytici používajú verejne dostupné satelitné snímky a mapovacie nástroje na monitorovanie oblastí záujmu. Google Earth sa napríklad používal na sledovanie odlesňovania, rozvoja miest a reakcie na katastrofy.

Niektoré operácie OSINT zahŕňajú tzv. **crowdsourcing**, kde dobrovoľníci prispievajú k zhromažďovaniu a analýze údajov. Projekty ako Bellingcat, čo je skupina investigatívnych novinárov, využívajú silu verejných príspevkov na odhaľovanie pravdy v zložitých prípadoch.